On Binomial Congruences; comprising an Extension of Fermat's and Wilson's Theorems, and a Theorem of which both are Special Cases.

By O. H. Mitchell,

Fellow in the Johns Hopkins University.

The complete theory of the binomial congruence $x^n \equiv D \bmod. k$ divides itself naturally into four parts. (1) The determination of n constitutes the theory of the periodicity of power residues;* (2) of x, the theory of the roots of the congruence; (3) of D, the theory of the number and the character of power residues; (4) of k, the theory of cyclotomic divisors, treated of in detail by Professor Sylvester in Vol. II., No. 4, of this Journal.

The theorems commonly known in the first three divisions of this subject have reference only to those numbers which are prime to the modulus. It is proposed in this article to so generalize certain fundamental theorems in (1), (2), and (3), including Fermat's and Wilson's, that they shall apply to all numbers, and to give a single theorem under which Fermat's and Wilson's theorems, thus extended, are both included as special cases.

§ 1. *Introductory Definitions and Notation.*

The number of numbers prime to and less than a given number, k, Professor Sylvester has named the *totient* of k, and, instead of the old symbol, $\phi(k)$, he uses $\tau(k)$ to designate it. In the following I shall speak of the number of numbers less than k, containing one and only one of its unequal prime factors, as the totient of k with respect to that prime factor. Thus, if $k = a^t b^v c^u$, where a, b, and c are prime numbers, I shall speak of the totient of k with respect to a, or the a-totient of k, and shall designate it by $\tau_a(k)$, in conformity with Professor Sylvester's notation. Likewise, the number of numbers less than k which contain a and b, but not c, I shall call the ab-totient of k, and write it $\tau_{ab}(k)$.

---

* *Power residues* is a term not used, I believe, but a needed translation of *Potenz-Reste.*

In general, representing by s the product of any given number of the unequal prime factors of a number, k, I shall speak of the s-totient of k, and denote it by $\tau_s(k)$. It is plain that, if $k = a^t b^u c^v$,

$$\tau_a(k) = a^{t-1}\tau(b^u c^v) = a^{t-1}b^{u-1}c^{v-1}(a-1)(c-1).$$

For there are $a^{t-1}b^u c^v$ numbers not greater than k which contain a, and, dividing these into a^{t-1} successive groups of $b^u c^v$ numbers each, we must reject from each group those numbers that contain either b or c, which leaves $a^{t-1}\tau(b^u c^v)$ numbers. In the same way it is plain that

$$\tau_{ab}(k) = a^{t-1}b^{u-1}\tau(c^v) = a^{t-1}b^{u-1}c^{v-1}(c-1).$$

We may write the different totients of $k = a^t b^u c^v$ in the following symmetrical manner, viz.:

$$\begin{aligned}
\tau_1(k) &= a^{t-1}b^{u-1}c^{v-1}(a-1)(b-1)(c-1),\\
\tau_a(k) &= \text{“} \quad (\ldots.)(b-1)(c-1),\\
\tau_b(k) &= \text{“} \quad (a-1)(\ldots.)(c-1),\\
\tau_c(k) &= \text{“} \quad (a-1)(b-1)(\ldots.),\\
\tau_{bc}(k) &= \text{“} \quad (a-1)(\ldots.)(\ldots.),\\
\tau_{ca}(k) &= \text{“} \quad (\ldots.)(b-1)(\ldots.),\\
\tau_{ab}(k) &= \text{“} \quad (\ldots.)(\ldots.)(c-1),\\
\tau_{abc}(k) &= \text{“} \quad (\ldots.)(\ldots.)(\ldots.).
\end{aligned}$$

The sum of these numbers is, of course, equal to k. This may readily be seen by noticing that the different terms of the expansion of

$$[\tau(a^t) + a^{t-1}][\tau(b^u) + b^{u-1}][\tau(c^v) + c^{v-1}]$$

are the above numbers, and this expression readily reduces to $a^t b^u c^v$. If $i =$ the number of unequal prime factors in any number, k, it is plain that the number of its different totients is 2^i.

It is convenient to have a name for those numbers whose enumeration makes up a totient of k. Professor Sylvester has called them, in the case of the ordinary totient, the *totitives* of k. Following this nomenclature, I shall be understood in speaking of the a-totitives, the ab-totitives, and, in general, of the s-totitives of k. X_s will conveniently denote *any* s-*totitive* of k. I shall use s throughout in the sense already defined, and shall use σ to denote the product of the same factors denoted by the s in the context, each factor, however, being

affected with the exponent which it has in k. Thus, if $k = a^t b^u \ldots . l^x \ldots . q^z$, and $s = ab \ldots . l$, then $\sigma = a^t b^u \ldots . l^x$. I shall use w frequently as $= ab \ldots . q$ = the product of all the unequal prime factors of k. I shall call a^t, b^u, etc., the *components* of k. Thus, we can define σ as the product of a certain number of the components of k, and s as the product of all the unequal prime factors of σ. If $s = 1$, then $\sigma = 1$.

§ 2. *On the Number and the Properties of the Roots of* $x^2 \equiv x$ *mod.* k.*

The solutions of $x^2 \equiv x \bmod. k$ have an important part in what follows, and will here be noticed somewhat in detail. This congruence breaks up into $x \equiv 0 \bmod. \sigma$ and $x - 1 \equiv 0 \bmod. \frac{k}{\sigma}$, where σ and $\frac{k}{\sigma}$ are prime to each other, since x and $x - 1$ are necessarily prime to each other. We may write $x \equiv 0 \bmod. \sigma$ as $x = \lambda\sigma$, whence the second congruence becomes $\lambda\sigma \equiv 1 \bmod. \frac{k}{\sigma}$. The last congruence gives one and only one value of λ less than $\frac{k}{\sigma}$, and, since $x = \lambda\sigma$, there is one and only one value of x corresponding to this value of λ which satisfies the congruence $x^2 \equiv x \bmod. k$. The x obtained in this way is plainly an s-totitive of k. Designate it by R_s. It is evident, now, that there are twice as many solutions of this congruence as there are ways of breaking up k into two factors prime to each other, viz.: 2^i where $i =$ the number of the components of k. Different separations give different solutions. For suppose $x = \lambda\sigma$, and $\lambda\sigma \equiv 1 \bmod. \frac{k}{\sigma}$ to have the same solution as $x = \lambda'\sigma'$ and $\lambda'\sigma' \equiv 1 \bmod. \frac{k}{\sigma}$. Then $\lambda\sigma$ is divisible by both σ and σ', and $\lambda\sigma - 1$ is divisible by both $\frac{k}{\sigma}$ and $\frac{k}{\sigma'}$. But $\lambda\sigma$ and $\lambda\sigma - 1$, differing by unity, are necessarily prime to each other. This gives $\sigma\sigma'$ prime to $\frac{k}{\sigma} \cdot \frac{k}{\sigma'}$, which is impossible if σ and σ' are different factors of k. Hence we have

THEOREM I. *The congruence* $x^2 \equiv x$ *mod.* k *has* 2^i *different roots, one root belonging to each of the* 2^i *classes of the totitives of* k.

If $k = a^t b^u c^v$, the eight solutions of the congruence may be denoted by R_1, R_a, R_b, R_c, R_{bc}, R_{ca}, R_{ab}, R_{abc}, the subscript denoting in each case to what class of totitives the root belongs. R_1 always $= 1$, found by solving $x \equiv 0 \bmod. 1$ and $x \equiv 1 \bmod. k$. R_w always $= 0$, found by solving $x \equiv 0 \bmod. k$ and $x \equiv 1 \bmod. 1$.

From $x^2 \equiv x \bmod. k$ we readily obtain $x^n \equiv x \bmod. k$. The solutions above

* In Serret's *Cours d'Algèbre Supérieure*, § 292, the solution of $x^2 \equiv 1 \bmod. k$ is discussed, a congruence which can be transformed into $x^2 \equiv x \bmod. k$ by substitution. I solve the latter congruence anew rather than transform results, both because its solution is simpler, and because the properties of its roots are more fundamental.

are, then, *repeating power residues* of the modulus k, and, in accordance with a suggestion from Professor Sylvester, are called the *repetents* of k.

I shall now prove some theorems in regard to the addition, subtraction, and multiplication of these repetents.

In all that follows I suppose s, s', s'', etc., to be prime to one another, unless otherwise stated.

THEOREM II. $R_s R_{s'} \equiv R_{ss'}$ *mod.* k.

We saw, in the course of the proof of Theorem I., that $R_s \equiv 0$ mod. σ, and $R_s \equiv 1$ mod. $\frac{k}{\sigma}$; that $R_{s'} \equiv 0$ mod. σ, and $R_{s'} \equiv 1$ mod. $\frac{k}{\sigma'}$; and that $R_{ss'} \equiv 0$ mod $\sigma\sigma'$ and $R_{ss'} \equiv 1$ mod. $\frac{k}{\sigma\sigma'}$. Whence $R_s R_{s'} \equiv 0 \equiv R_{ss'}$ mod. $\sigma\sigma'$, and $R_s R_{s'} \equiv 1 \equiv R_{ss'}$ mod. $\frac{k}{\sigma\sigma'}$. $\therefore R_s R_{s'} \equiv R_{ss'}$ mod. k. Q. E. D.

COROLLARY. $R_{ss'} R_{ss''} \equiv R_{ss's''}$ mod. k, since $R_s R_s \equiv R_s$ mod. k.

THEOREM III. $R_s + R_{s'} \equiv R_{ss'} + 1$ mod. k.

For $R_s - 1 \equiv 0$ mod. $\frac{k}{\sigma}$ and $R_{s'} - 1 \equiv 0$ mod. $\frac{k}{\sigma'}$, and by multiplication,

$$(R_s - 1)(R_{s'} - 1) \equiv 0 \equiv R_s R_{s'} - R_s - R_{s'} + 1 \text{ mod. } k.$$

$$\therefore R_s + R_{s'} \equiv R_{ss'} + 1 \text{ mod. } k.$$

COROLLARY 1. $R_s + R_{s'} \equiv 1$ mod. k when $ss' = w$, for then $R_{ss'} \equiv 0$ mod. k.

COROLLARY 2. $R_{ss'} + R_{ss''} \equiv R_{ss's''} + R_s$ mod. k. *Hence, the sum of any two of the repetents of* k *is congruous to the sum of any other two, provided the product of the subscripts is the same for each sum.*

COROLLARY 3. $(R_s - R_{s'})^2 \equiv 1 - R_{ss'}$ mod. k, and when $ss' = w$, then $R_{ss'} \equiv 0$, and we have $(R_s - R_{s'})^2 \equiv 1$ mod. k, obtained by squaring and reducing. $R_s - R_{s'}$ is, then, a root of $x^2 \equiv 1$ mod. k, in conformity with the relation existing between the algebraic roots of $x^2 = x$ and $x^2 = 1$. In general, $R_s - R_{s'}$ is a root of $X^2 \equiv R_{\overline{ss'}}$ mod. k, where $\overline{ss'} = \frac{w}{ss'}$.

THEOREM IV. $R_s - R_{s'} \equiv R_{ms} - R_{ms'}$ mod. k, m being any product of the unequal prime factors of k which is prime to s and s', and the relation holds whether s and s' are prime to each other or not. In words, *The residue mod.* k, *of the difference of any two of the repetents of* k *remains constant if their subscripts be both multiplied by any prime factor or factors not contained in either, or both divided by any prime factor or factors common to both.* For, by Theorem III., Corollary 2,

$$R_s + R_{ms'} \equiv R_{s'} + R_{ms} \text{ mod. } k.$$

The most general theorem of summation may be stated as follows, viz.:—

THEOREM V. *The modulus being* k, *the sum of a given number of repetents is congruous to the sum of the same number of any other repetents, provided only that the product of all the subscripts is the same in each sum.*

For any sum of n repetents may plainly be transformed, by Theorem III., Corollary 2, in such a way that the first term will have for its subscript only those letters which occur in all the n terms. If there be no letters which occur in all the n terms, the first term may be transformed into R_1. The second term may be made to have for its subscript, in addition to those contained in the first term, only those letters which occur in the remaining $(n-1)$ terms, and so on, till the last term whose subscript contains all the different letters of the preceding terms, together with any which may occur in only one of the terms. Thus,

$$R_{cdf} + R_{cde} + R_f + R_{cf} + R_{ef} + R_{bcf} + R_{def} + R_{abc} \equiv R_1 + R_1 + R_f + R_{cf} + R_{cf} + R_{cf} + R_{bcdef} + R_{abcdef} \text{ mod. } a^t b^u c^v d^w e^x f^y$$

by such a transformation. The number of terms remains the same and the product of the subscripts remains the same. Evidently, every sum of terms which fulfils the given conditions can be reduced to the same sum. Hence the theorem is proved.

COROLLARY 1. $R_s + R_{s'} + \ldots + R_{s^{[n]}} \equiv R_{ss's''\ldots s^{[n]}} + nR_1 \text{ mod. } k.$

COROLLARY 2. $\Sigma R_{ss's''\ldots s^{[r]}} \equiv C_r^n R_{ss's''\ldots s^{[n]}} + C_{r+1}^n \text{ mod. } k$, where C_r^n denote the r^{th} coefficient of the n^{th} power of a binomial. The first member of the congruence denotes the sum of those repetents whose subscripts are the C_{r+1}^{n+1} combinations of the $(n+1)$ S's taken $(r+1)$ at a time.

COROLLARY 3. If $k = a^t b^u \ldots q^z$, we have

$$R_1 + \Sigma R_a + \Sigma R_{ab} + \ldots + \Sigma R_{ab\ldots p} + R_{ab\ldots q} \equiv 2^{i-1} \text{ mod. } k,$$

where $i =$ the number of the components of k. And also

$$R_1 - \Sigma R_a + \Sigma R_{ab} - \Sigma R_{abc} + \ldots (-)^i R_{ab\ldots q} \equiv 0 \text{ mod. } k.$$

If we write $\bar{s}$ to denote briefly $\frac{w}{s}$, where w is the product of all the unequal prime factors of the modulus, k, we shall have a convenient notation for expressing certain formulæ which will be most useful further on. As before, let s, s', s'', etc., be prime to one another, but of course $\bar{s}, \bar{s'}, \bar{s''}$ will not be so. It is to be remembered that R_s contains only those factors of k which are found in s, whereas $R_{\bar{s}}$ contains only those *not* found in s, so that the dash over s has the significance of a logical negative.

$$(A) \qquad R_{\bar{s}} R_{\bar{s}'} \equiv 0 \text{ mod. } k.$$

$$(B) \qquad R_{\bar{s}} + R_{\bar{s}'} \equiv R_{\overline{ss'}} \text{ mod. } k.$$

$$(C) \qquad \Sigma_0^n R_{\bar{s}} \equiv R_{\overline{ss's''\ldots s^{[n]}}} \text{ mod. } k.$$

$$(D) \qquad \Sigma R_{\overline{ss's''\ldots s^{[r]}}} \equiv C_r^n R_{\overline{ss's''\ldots s^{[n]}}} \text{ mod. } k.$$

$$(E) \qquad R_{\bar{s}} - R_{\bar{s}'} \equiv -(R_s - R_{s'}) \text{ mod. } k.$$

(A) follows, since $\frac{w}{s} \cdot \frac{w}{s'}$ contains w. (B) is only Corollary 2, Theorem III., in another form. (C) follows directly from (B), and (D) from (C).

THEOREM VI. If $X \equiv \alpha R_{\bar{s}} + \beta R_{\bar{s}'} + \ldots. + \lambda R_{\overline{s^{[n]}}}$ mod. k, and $X' \equiv \alpha' R_{\bar{s}} + \beta R_{\bar{s}'} + \cdots + \lambda' R_{\overline{s^{[n]}}}$, and so on, for X'', X''', etc., where $\alpha, \beta, \ldots. \alpha', \beta', \ldots.$ are any integers, then

$$(XX'X''\ldots.) \equiv (\alpha\alpha'\alpha''\ldots.) R_{\bar{s}} + (\beta\beta'\beta''\ldots.) R_{\bar{s}'} + \ldots. + (\lambda\lambda'\lambda'') R_{\overline{s^{[n]}}} \text{ mod. } k.$$

For since $R_{\bar{s}} R_{\bar{s}'} \equiv 0$, all cross multiplication will give terms congruous to zero.

COROLLARY. If $X \equiv \alpha R_{\bar{s}} + \beta R_{\bar{s}'} + \ldots. + \lambda R_{\overline{s^{[n]}}}$ mod. k, as before, then $X^m \equiv \alpha^m R_{\bar{s}} + \beta^m R_{\bar{s}'} + \ldots. + \lambda^m R_{\overline{s^{[n]}}}$ mod. k.

THEOREM VII.* *If* $X \equiv \alpha R_{\bar{a}} + \beta R_{\bar{b}} + \ldots. + \chi R_{\bar{q}}$ *mod.* $k = a^t b^u \ldots. q^z$, *then* $X \equiv \alpha$ *mod.* a^t, $X \equiv \beta$ *mod.* b^u, *etc., and, vice versa, if* $X \equiv \alpha$ *mod.* a^t, $X \equiv \beta$ *mod.* $b^u, \ldots.$ *and* $X \equiv \chi$ *mod.* q^z, *then* $X \equiv \alpha R_{\bar{a}} + \beta R_{\bar{b}} + \ldots. + \chi R_{\bar{q}}$ *mod.* $k = a^t b^u \ldots. q^z$. These results follow from the definition of the repetents, $R_{\bar{a}}$, $R_{\bar{b}}$, etc.

THEOREM VIII. *If* $AR_{\bar{a}} + BR_{\bar{b}} + \ldots. + QR_{\bar{q}} \equiv A'R_{\bar{a}} + B'R_{\bar{b}} + \ldots. + Q'R_{\bar{q}}$ *mod.* $k = a^t b^{t'} \ldots. q^{t''}$, *then* $A \equiv A'$, $B \equiv B', \ldots.$, *mod.* k. This follows from the definition of $R_{\bar{a}}$, $R_{\bar{b}}$, etc. [See Dirichlet's *Zahlentheorie*, § 25.]

THEOREM IX. *If* $f(X) \equiv 0$ *mod.* $k = a^t b^{t'} \ldots. q^{t''}$ *be transformed by the substitution* $X \equiv uR_{\bar{a}} + vR_{\bar{b}} + \ldots. + yR_{\bar{q}}$, *it becomes* $f(u) R_{\bar{a}} + f(v) R_{\bar{b}} + \ldots. + f(y) R_{\bar{q}} \equiv 0$ *mod.* k, *which involves* $f(u) \equiv 0$ *mod.* a^t, $f(v) \equiv 0$ *mod.* $b^{t'}$, *etc.* This is obvious from Theorem VII.

THEOREM X. *If* N_s *be any number which contains* σ, *then* $R_s N_s \equiv N_s$ *mod.* k. For $R_s \equiv 1$ mod. $\frac{k}{\sigma}$.

I give below the repetents of the modulus 210, for the convenience of any reader who may wish to illustrate the preceding theorems by examples.

---

* In Dirichlet's *Zahlentheorie*, § 25, this solution of a system of linear congruences is given. $Aa', Bb', \ldots.$ are used instead of $R_{\bar{a}}, R_{\bar{b}}, \ldots.$, where $A = \frac{k}{a^t}$, $B = \frac{k}{b^u}, \ldots.$, and $a', b', \ldots.$, are to be determined in such a way that $Aa' \equiv 1$ mod. a^t, $Bb' \equiv 1$ mod. b', etc., etc. These conditions are the same as those which, as we have seen, the repetents $R_{\bar{a}}, R_{\bar{b}}, \ldots.$ fulfil.

Mod. $210 = 2 . 3 . 5 . 7.$

$R_1 = 1$	$R_2 = 106$ $R_3 = 141$ $R_5 = 85$ $R_7 = 91$	$R_{2.3} = 36$ $R_{2.5} = 190$ $R_{2.7} = 196$ $R_{3.5} = 15$ $R_{3.7} = 21$ $R_{5.7} = 175$	$R_{3\ 5.7} = 105$ $R_{5.7.2} = 70$ $R_{7.2.3} = 126$ $R_{2.3.5} = 120$	$R_{2.3\ 5.7} = 0$

§ 3. *Fermat's and Wilson's Theorems.*

On examination of a table of power residues for a given modulus, it will be seen that all the repetents of the modulus play the same part in the table as unity. Thus, in the following table,

Mod. 15.

Natural Numbers	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Quad. Residues .	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1
Cubic Residues .	0	1	8	12	4	5	6	13	2	9	10	11	3	7	14
Biquad. Residues	0	1	1	6	1	10	6	1	1	6	10	1	6	1	1

the repetents 0, 6, and 10 have a part similar to that of unity, which is itself one of the four repetents of 15. These numbers which we have called repetents are, in fact, a kind of residual units. Their fundamental property, $R_s^n \equiv R_s \bmod. k$, shows their analogy to ordinary unity, and Theorem II., which gives the product of two repetents congruous to a certain third one, shows their analogy to the multiple units of quaternions, where we have $ij = k$. Their analogy to the double units of imaginary or complex quantities is seen in Theorems VIII. and IX.

It will now seem almost obvious that Fermat's, Wilson's, and other theorems in power residues ought to be extensible in such a way that all these repetents, or residual units, shall have the same part as unity has in the present forms of the theorems. It will now be shown that such is the case.

Extension of Fermat's Theorem for Composite Moduli. $X_s^{\tau_s(k)} \equiv R_s \bmod. k$. For a proof I generalize one of the proofs of the ordinary theorem. Let $\alpha, \beta, \gamma, \ldots . \omega$ be the $\tau_s(k)$ s-totitives of k. Multiply each member of the group by any one, as ρ. The series then becomes $\alpha\rho, \beta\rho, \gamma\rho, \ldots . \omega\rho$. No two members of this latter series are congruous mod. k, for $(\theta - \delta)\rho$ cannot contain k. The

numbers are still s-totitives of k, for no new factor has been introduced by the multiplication. The numbers of the second series are, therefore, taken in some order, congruous respectively to the numbers of the first series, and we have $(\alpha\beta \ldots . \omega)\rho^{\tau_s(k)} \equiv \alpha\beta \ldots . \omega \bmod. k$, or $(\alpha\beta \ldots . \omega)(\rho^{\tau_s(k)} - 1) \equiv 0 \bmod. k$. $\therefore \rho^{\tau_s(k)} \equiv 1 \bmod. \frac{k}{\sigma}$. But $R_s \equiv 1 \bmod. \frac{k}{\sigma}$ [Theorem I.], $\therefore \rho^{\tau_s(k)} \equiv R_s \bmod. \frac{k}{\sigma}$. Both sides of this last congruence evidently contain σ, for $R_s = \lambda\sigma$ [Theorem I.], and the unequal prime factors in ρ evidently cannot have smaller exponents in $\rho^{\tau_s(k)}$ than they have in σ. $\therefore \rho^{\tau_s(k)} \equiv R_s \bmod. k$, or, writing X_s for ρ,

$$X_s^{\tau_s(k)} \equiv R_s \bmod. k. \quad \text{Q. E. D.}$$

For $s = 1$, we have $R_s = 1$, and $x^{\tau(k)} \equiv 1 \bmod. k$, — the ordinary form of the Fermatian theorem for composite moduli, in which x is supposed prime to k. This is now seen to be only one of the 2^i different cases of the extended theorem.

I now give another proof dependent upon the ordinary theorem.

Let $k = a^t b^u \ldots . l^x m^y \ldots . q^z$, and $s = ab \ldots . l$. If $X_s \equiv a' \bmod. a^t$, $X_s \equiv b' \bmod. b^u, \ldots . X_s \equiv q' \bmod. q^z$, then $X_s \equiv a'R_{\bar{a}} + b'R_{\bar{b}} + \ldots . + q'R_{\bar{q}} \bmod. k$ [§ 2, Theorem VII.].

$$\therefore X^n \equiv a'^n R_{\bar{a}} + b'^n R_{\bar{b}} + \ldots . + q'^n R_{\bar{q}} \bmod. k \text{ [§ 2, Theorem VI.]};$$

$$\therefore \text{If } n = \tau_s(k),\ X^{\tau_s(k)} \equiv R_{\bar{m}} + \ldots . + R_{\bar{q}} \equiv R_{\overline{m \ldots . q}} = R_s \bmod. k.$$

For, from the linear congruences, a' contains a, b' contains $b, \ldots . l'$ contains l, m' is prime to $m^y, \ldots .$ and q' prime to q^z. Hence $a'^{\tau_s(k)} R_{\bar{a}} \equiv 0 \bmod. k, \ldots . l'^{\tau_s(k)} R_{\bar{l}} \equiv 0 \bmod. k$, $m'^{\tau_s(k)} \equiv 1 \bmod. m^y, \ldots .$ and $q'^{\tau_s(k)} \equiv 1 \bmod. q^z$, $\tau_s(k)$ containing $\tau(m^y), \ldots .$, and $\tau(q^z)$. We have $R_{\bar{m}} \ldots . R_{\bar{q}} \equiv R_{\overline{m \ldots . q}} \bmod. k$, by § 2, Formula (C).

This method of proof especially brings out the analogy between this theorem and De Moivre's theorem concerning the n^{th} roots of unity.

Examples. If $k = 210 = 2.3.5.7$ [see table in last section], $R_{2.3} = 36$, and $X_{2.3}^{24} \equiv 36 \bmod. 210$, where $X_{2.3}$ is any 2.3-totitive of 210, i. e. any number which contains both 2 and 3, but *not* 5 or 7. So $X_{2.3.5}^{6} \equiv 120 \bmod. 210$, where $X_{2.3.5}$ is any number that contains 2, 3, and 5, but not 7, etc.

Whatever has been proved, Theorems II. to X. in regard to R_s, may now be stated in terms of $X_s^{\tau_s(k)}$. For instance, Corollary 3, Theorem VI., becomes, since $\tau(k)$ is a multiple of $\tau_s(k)$,

$$X_1^{\tau(k)} + \Sigma X_a^{\tau(k)} + \Sigma X_{ab}^{\tau(k)} + \ldots . + X_{ab \ldots . q}^{\tau(k)} \equiv 2^{i-1} \bmod. k.$$

The original theorem of Fermat, for prime numbers, may be regarded as a special case of this last congruence, for when k is prime, $2^{i-1} = 1$, and we have $X_1^{\tau(k)} \equiv 1 \bmod. k$.

If we designate by $\Pi_s(k)$ the product of the $\tau_s(k)$ s-totitives of k, we may state

An Extension of Wilson's Theorem for Composite Moduli. $\Pi_s(k) \equiv R_s$ *mod.* k, *except when* $\frac{k}{\sigma}$ *is a power of an odd prime number, double such a power, or* $= 4$, *and* $\frac{\sigma}{s}$ *is at the same time an odd number, in all of which cases* $\Pi_s(k) \equiv -R_s$ *mod.* k.

Proof. Since $\tau_s(k) = \frac{\sigma}{s}\tau\left(\frac{k}{\sigma}\right)$, we may divide the s-totitives of k into $\frac{\sigma}{s}$ groups of $\tau\left(\frac{k}{\sigma}\right)$ each, and may write the theorem to be proved as follows: —

$$s^{\tau_s(k)}\left[\Pi_1\left(\frac{k}{\sigma}\right)\right]\left[\Pi_1\left(\frac{k}{\sigma}\right), \text{ each} + \frac{k}{\sigma}\right]\left[\Pi_1\left(\frac{k}{\sigma}\right), \text{ each} + \frac{2k}{\sigma}\right]\left[\ldots\right]$$

$$\left[\Pi_1\left(\frac{k}{\sigma}\right), \text{ each} + \left(\frac{\sigma}{s} - 1\right)\frac{k}{\sigma}\right] \equiv \pm R_s \bmod. k.$$

We have here $\tau_s(k)$ numbers less than k, and no two of them are congruous; for suppose $ls + \lambda\frac{ks}{\sigma} \equiv ms + \mu\frac{ks}{\sigma}$ mod. k, where l and m are prime totitives of $\frac{k}{\sigma}$. This may be written $(l - m)s \equiv (\mu - \lambda)\frac{ks}{\sigma}$ mod. k, which is impossible, since the right member is divisible by $\frac{k}{\sigma}$ and the left is prime to $\frac{k}{\sigma}$.

R_s contains σ by Theorem I., and $\tau_s(k)$ is plainly in no case smaller than any exponent in σ. Therefore both sides contain σ whatever may be the sign of R_s. If $\frac{k}{\sigma}$ be a power of an odd prime number, double such a power, or $= 4$, each parenthesis is congruous to -1 mod. $\frac{k}{\sigma}$. If, further, $\frac{\sigma}{s}$ be at the same time an odd number, the product of all the parentheses is congruous to -1 mod. $\frac{k}{\sigma}$. In all other cases the product of the parentheses is congruous to $+1$ mod. $\frac{k}{\sigma}$. The congruence to be proved reduces, then, to $\pm s^{\tau_s(k)} \equiv \pm 1$ mod. $\frac{k}{\sigma}$, and, if 1 be taken with the same sign as the left-hand member, this is a valid congruence by the Fermatian theorem. Hence, the original congruence being valid for both mod. σ and mod. $\frac{k}{\sigma}$, it is valid for mod. k. Q. E. D.

Another proof of this theorem is as follows: Let $k = a^t b^u \ldots . l^x m^y \ldots . q^z$, and $s = ab \ldots . l$. Then if $X_s' \equiv a'$ mod. $a^t \ldots . X_s' \equiv q'$ mod. q^z, and $X_s'' \equiv a''$ mod. $a^t \ldots . X_s'' \equiv q''$ mod. q^z, and so on for X''', etc.;

$$X_s' \equiv a'R_{\bar{a}} + b'R_{\bar{b}} + \ldots . + q'R_{\bar{q}} \bmod. k,$$
$$X_s'' \equiv a''R_{\bar{a}} + b''R_{\bar{b}} + \ldots . + q''R_{\bar{q}} \quad " \quad "$$

and so on for X_s''', etc., all the $\tau_s(k)$ s-totitives of k being obtained in this way, since there are a^{t-1} terms, a', a'', etc., b^{u-1} terms, b', b'', etc., l^{x-1} terms, l', l'', etc., $\tau(m^y)$ terms, m', m'', etc., and $\tau(q^z)$ terms, q', q'', ..., and the product of these numbers $= a^{t-1}b^{u-1}. \ldots . l^{x-1}\tau(m^y) \ldots . \tau(q^z) = \tau_s(k)$. Then we have

$$\Pi_s(k) \equiv \left(m'm''. \ldots . m^{[\tau(m^t)]}\right)^{\frac{\tau_s(k)}{\tau(m^y)}} R_{\bar{m}} + \ldots . + \left(q'q'' \ldots . q^{[\tau(q^z)]}\right)^{\frac{\tau_s(k)}{\tau(q^z)}} R_{\bar{q}}$$

$$\therefore \Pi_s(k) \equiv \left(-1\right)^{\frac{\tau_s(k)}{\tau(m^y)}} R_{\bar{m}} + \ldots . + \left(-1\right)^{\frac{\tau_s(k)}{\tau(q^z)}} R_{\bar{q}} \text{ mod. } k.$$

$$\frac{\tau^s(k)}{\tau(m^y)} = \frac{\sigma}{s}\tau\left(\frac{k}{m^y\sigma}\right), \ldots . \text{ and } \frac{\tau_s(k)}{\tau(q^z)} = \frac{\sigma}{s}\tau\left(\frac{k}{q^z\sigma}\right),$$

which are even numbers, except when $\frac{k}{\sigma}$ is a power of an odd prime number, double such a power, or $= 4$, and $\frac{\sigma}{s}$ is at the same time an odd number. Hence, outside of the excepted cases, we have

$$\Pi_s(k) \equiv R_{\bar{m}} + \ldots . + R_{\bar{q}} \equiv R_{\overline{m \ldots . q}} = R_s \text{ mod. } k,$$

[see § 2, Formula (C)]. For $\frac{\sigma}{s}$ odd, and $\frac{k}{\sigma} = q^z$, where q is an odd prime number, or where $q^z = 4$, we have $\Pi_s(k) \equiv -R_{\bar{q}} = -R_s$ mod. k. For $\frac{\sigma}{s}$ odd, and $\frac{k}{\sigma} = 2q^z$, where q is an odd prime number, we have

$$\Pi_s(k) \equiv \left(-1\right)^{\frac{\sigma}{s}\tau\left(\frac{k}{2\sigma}\right)} R_{\bar{2}} + \left(-1\right)^{\frac{\sigma}{s}\tau\left(\frac{k}{q^z\sigma}\right)} R_{\bar{q}} \text{ mod. } k.$$

$\therefore \Pi_s(k) \equiv + R_{\bar{2}} - R_{\bar{q}}$ mod. k. But when $k =$ twice an odd number, as in this case, we plainly have $R_{\bar{2}} = \frac{1}{2}k$, and therefore $R_{\bar{2}} \equiv -R_{\bar{2}}$ mod. k; so that $\Pi_s(k) \equiv -R_{\bar{2}} - R_{\bar{q}} \equiv -R_{\overline{2q}} = -R_s$ mod. k, according to § 2, Formula (C). Q. E. D.

Examples. If $k = 60 = 2^2 . 3 . 5$, then $R_{2.3} = 36$, $R_{2.5} = 40$, and $R_{3.5} = 45$. We have, therefore,

$$\Pi_{2.3}(60) \equiv \quad 36 \text{ mod. } 60, \text{ i. e. } 6 . 12 . 18 . 24 . 36 . 42 . 48 . 54 \equiv 36,$$
$$\Pi_{2.5}(60) \equiv \quad 40 \text{ " " " } 10 . 20 . 40 . 50 \equiv 40,$$
$$\Pi_{3.5}(60) \equiv -45 \text{ " " " } 15 . 45 \equiv -45,$$

the sign of the right-hand member in the last congruence being negative, since $\frac{k}{\sigma} = \frac{60}{3.5} = 4$, and $\frac{\sigma}{s} = \frac{15}{3.5} = 1$.

For $s = 1$, we have, of course, $\Pi_1(60) \equiv 1$ mod. 60.

We may now state Theorems II. to X. in terms of $\Pi_s(k)$, care being taken in regard to signs. For instance, Theorem II. now becomes

$$\Pi_s(k)\,\Pi_{s'}(k) \equiv \pm\, \Pi_{ss'}(k) \text{ mod. } k,$$

the sign of the right-hand member being determined according to the previous theorem.

§ 4. *The Periodicity of Power Residues.*

THEOREM I. *Every power residue of an* s*-totitive of* k, X_s, *is also an* s*-totitive of* k. For if D be an n^{th} power residue of X_s mod. k, we have $X_s^n - D = \lambda k$, from which we see that D contains s and is prime to $\frac{k}{\sigma}$, and is therefore an s-totitive of k, for, otherwise, we should have in each case the difference of two integers equal to a fraction.

THEOREM II. If $k = a^t b^u \ldots . l^y \ldots . q^z$, $\sigma = a^t b^u \ldots . l^y$, $X_s = \lambda a^{t'} b^{u'} \ldots . l^{y'}$ where λ is prime to k, and $v - v'$ be the greatest difference obtained by subtracting each of the exponents $t', u', \ldots . y'$, from $t, u, \ldots . y$, respectively, and ϕ = the number of integers in $\frac{v + v' - 1}{v'}$, then

The ϕ^{th} *and all higher power residues of* X_s *mod.* k *contain* σ, *and no power residue of less degree than* ϕ *contains* σ.

Since a divisor of two numbers divides their remainder after division, we have only to consider what value of n will render X_s^n divisible by σ, i. e. by $a^t b^u \ldots . l^y$; then, since $v'\phi =$ or $> v$, and $v'(\phi - 1) < v$, the theorem is proved.

THEOREM III. *The power residues mod.* k *of any number* X_s *occur periodically as the degree of the power increases; and the exponent of the period is a divisor of* $\tau_s(k)$.

No power residue (except R_s) can occur twice as the degree increases, unless R_s intervenes; for if $X_s^n \equiv X_s^{n+h}$ mod. k without any intermediate power congruous to R_s, it follows at once, by multiplying both sides of the congruence repeatedly by X_s, that no power residue is congruous to R_s, which is not true, for $X_s^{\tau_s(k)} \equiv R_s$ mod. k by the extended Fermatian Theorem.

Let X_s^δ be the lowest power of X_s which is congruous to R_s. We have, then, $X_s^\delta \equiv R_s$ mod. k, and, by squaring, $X_s^{2\delta} \equiv R_s$ mod. k, whence $X_s^{\delta+h} \equiv X_s^{2\delta+h}$ mod. k, h being any positive integer. This shows that from the δ^{th} degree upwards the power residues of X_s mod. k recur in the same order in periods of δ numbers each. But, according to the preceding theorem, the first $(\phi - 1)$ residues of the first period are different from the corresponding residues in the higher periods. The remaining $\delta - \phi + 1$ residues of the first period are the same as the corresponding residues in the second, third, and higher periods;

for, by multiplying together, member by member, $X_s^{\phi+h} \equiv X_s^{\phi+h} \bmod. k$ and $X_s^{\delta} \equiv R_s \bmod. k$, we obtain $X_s^{\delta+\phi+h} \equiv X_s^{\phi+h} \bmod. k$, since $R_s X_s^{\phi+h} \equiv X_s^{\phi+h} \bmod. k$ by Theorem X. in § 2.

When $\phi = 1$, i. e. when all the exponents of the unequal prime factors common to X_s and k are as great in X_s as in k, then the first period of the power residues of X_s is the same as the higher periods.

It is evident now that δ is a divisor of $\tau_s(k)$, for R_s occurs only at the end of each period of residues, and $X_s^{\tau_s(k)} \equiv R_s \bmod. k$.

THEOREM IV. *The numbers given by the formula* $\mathrm{X_s} + \frac{\mathrm{sk}}{\sigma}\mathrm{y}$, *where* $\mathrm{y} =$ *any integer, have the same power residues in the same order beyond the* $(\mathrm{t}-1)^{th}$ *degree,* t *being the greatest exponent in* σ. *There are* $\frac{\sigma}{\mathrm{s}}$ *such numbers less than* k.

Proof. If X_s be any s-totitive of k, then all the s-totitives of k are included among the residues of $X_s + s\lambda$, where λ is any integer from 0 to $\frac{k}{s} - 1$. Let us consider for what values of λ, if for any, $X_s^n \equiv (X_s + s\lambda)^n \bmod. k$, for all values of $n =$ or $> t$. Transposing and taking out the factor s^n, we have $s^n\{(Q+\lambda)^n - Q^n\} \equiv 0 \bmod. k$, where Q denotes $\frac{X_s}{s}$. Therefore, if $n =$ or $> t$, the largest exponent in σ, we have $(Q+\lambda)^n - Q^n \equiv 0 \bmod. \frac{k}{\sigma}$. Since λ is a factor of the left-hand member, the congruence will be satisfied by making $\lambda = \frac{k}{\sigma}y$, where y is any integer; and it may be shown that the congruence will not hold if λ is prime to any prime factor of $\frac{k}{\sigma}$, say p, for then $(Q+\lambda)^n \equiv Q^n \bmod. p$, which is not true for *all* values of $n =$ or $> t$, $\frac{k}{\sigma}$ being prime to X_s, and p therefore prime to Q.

Substituting then $\frac{k}{\sigma}y$ for λ, we have $X^n \equiv \left(X_s + \frac{sk}{\sigma}y\right)^n \bmod. k$. Q. E. D.

There are plainly $\frac{\sigma}{s}$ numbers less than k which have the same power residues in the same order beyond the $(t-1)^{\text{th}}$ power, for, giving y all values from 0 to $\frac{\sigma}{s} - 1$ in the formula, $X_s + \frac{sk}{\sigma}y$, we get $\frac{\sigma}{s}$ different numbers whose residues mod. k are all different.

Those numbers obtained by giving to y values prime to $\frac{\sigma}{s}$ contain the prime factors of s only to the first degree, and therefore the value of ϕ (see Theorem II.) for these numbers is t, the greatest exponent in σ. Hence for $n < t$ there will be a disagreement among the power residues of the numbers given by the formula $X_s + \frac{sk}{\sigma}y$.

Example. If $k = 360 = 2^3 . 3^2 . 5$, the four numbers less than k given by the formula $2 + \frac{360}{2^2} y$ all have the same power residues beyond the second power. Also the numbers, $14 + \frac{360}{2^2} y$. Also the numbers, $42 + \frac{360}{2^2 . 3} y$, and there are $\frac{2^3 . 3^2}{2 . 3} = 12$ of these less than k.

Since $\tau_s(k) = \frac{\sigma}{s} \tau_1 \left(\frac{k}{\sigma}\right)$, we see that the s-totitives of k have only $\tau_1 \left(\frac{k}{\sigma}\right)$ different periods of power residues. If $s = 1$, then $\sigma = 1$, and $X_s + \frac{sk}{\sigma} y$ gives only one number less than k, viz. X_1, and there are in this case $\tau_1(k)$ different periods of power residues.

§ 5. *The Number of Roots of* $X^n - R_s \equiv 0$ *mod.* k.

Let $k = a^t b^{t'} \ldots . l^{t''} m^{t'''} \ldots . q^{t^{IV}}$, and $s = ab \ldots . l$. Then $\sigma = a^t b^{t'} \ldots . l^{t''}$. If $\theta =$ the number of integers in $\frac{t + n - 1}{n}$, $X^n - R_s \equiv 0 \bmod a^t$ has $a^{t-\theta}$ roots, for, since $n\theta =$ or $> t$, and $n(\theta - 1) < t$, the n^{th} powers of all those numbers (and of no others) which contain a^θ will contain a^t, i. e. all such numbers will satisfy $X^n - R_s \equiv 0 \bmod. a^t$, and there are $a^{t-\theta}$ of such numbers less than a^t. In the same way $X^n - R_s \equiv 0 \bmod. b^{t'}$ has $b^{t'-\theta'}$ roots, etc. Hence $X^n - R_s \equiv 0 \bmod. \sigma$ has $a^{t-\theta} b^{t'-\theta'} \ldots . l^{t''-\theta''}$ roots [Serret, *Alg. Sup.* § 325].

Since $R_s \equiv 1 \bmod. \frac{k}{\sigma}$, $X^n - R_s \equiv 0 \bmod. m^{t'''}$ has μ roots, where μ is the g. c. d. of n and $\tau(m^{t'''})$ [Serret, *Alg. Sup.* § 322], and χ roots mod. $q^{t^{IV}}$, where χ is the g. c. d. of n and $\tau(q^{t^{IV}})$. Hence $X^n - R_s \equiv 0 \bmod. \frac{k}{\sigma}$ has $\mu \ldots . \chi$ roots. In case one of the prime factors of $\frac{k}{\sigma}$, as $m_1 = 2$, we have, when n is even and $m^{t^{IV}} > 4$, $\mu =$ double the g. c. d. of n and $\frac{1}{2}\tau(m^{t^{IV}})$ [Serret, *Alg. Sup.* § 325].

Hence we have that $X^n - R_s \equiv 0 \bmod. k$ has $a^{t-\theta} b^{t'-\theta'} \ldots . l^{t''-\theta''} \mu \ldots . \chi$ roots.

If $n =$ or $>$ than any of the exponents in σ, then the number of roots becomes $a^{t-1} b^{t'-1} \ldots . l^{t''-1} \mu \ldots . \chi$.

If we denote any repetent of k by R without a subscript, then the whole number of roots of $X^n - R \equiv 0 \bmod. k$ is

$$(\alpha + a^{t-\theta})(\beta + b^{t'-\theta'}) \ldots . (\chi + q^{t^{IV}-\theta^{IV}}),$$

for the different terms of this expansion are, by what has just been given, the numbers of roots for the different values of the repetents $R_1, R_a, R_b, \ldots . R_{ab}$,

$R_{bc}, \ldots . R_{abc}, \ldots . R_{ab\ldots q}$, there being the same number of terms as there are values of R, viz. 2^i, where $i =$ the number of the components of k.

Example. If $k = 72 = 2^3 . 3^2$, $X^n - R \equiv 0$ mod. 72 has

for $n = 2$, $(4 + 2)(2 + 3) = 30$ roots,
" $n = 3$, $(1 + 2^2)(3 + 3) = 30$ "
" $n = 4$, $(4 + 2^2)(2 + 3) = 40$ "
" $n = 5$, $(1 + 2^2)(1 + 3) = 20$ "
" $n = 6$, $(4 + 2^2)(6 + 3) = 72$ "

or, in other words, all the 6th-power residues of 72 are repetents. This number, 6, I shall call the period of the modulus 72. In general, the least value of n for which all the power residues become repetents of the modulus, k, I shall call the period of the modulus, k, and shall designate it by $P(k)$. The formula given for the number of the roots of $X^n - R \equiv 0$ mod. k shows us that $P(k)$ = the least common multiple of $\tau(a^t)$, $\tau(b^{t'})$, etc. For α, β, etc., then become $\tau(a^t)$, $\tau(b^{t'})$, etc., and the formula becomes

$$[\tau(a^t) + a^{t-1}][\tau(b^{t'}) + b^{t'-1}] \ldots . [\tau(q^{t^{IV}}) + q^{t^{IV}-1}] = k.$$

The $P(k)^{th}$ powers of all the numbers prime to k are congruous to R_1, i. e. to unity, mod. k, as is shown in Serret's *Cours d'Algèbre Supérieure, tome* 2, *page* 51.

It will be noticed by examination of the different totients of k, given in § 1, that $\tau_s(k)$ is in every case either a divisor or a multiple of $P(k)$.

§ 6. *The Number of Roots of* $X^n - D \equiv 0$ *mod.* k.

D is supposed to be any n^{th}-power residue. Consider, first, the congruence $X^n - D \equiv 0$ mod. a^t. Divide the numbers represented by D into the following classes, viz.: (1) those prime to a^t; (2) those containing a^n and no higher power of a; (3) those that contain a^{2n} and no higher power of a; and so on, to lastly those that contain $a^{\theta n}$, where $\theta = E\left(\frac{t+n-1}{n}\right)$, as in last section. Obviously all the n^{th}-power residues are included in this classification. We have, then, that the number of roots of $X^n - D \equiv 0$ mod. a^t is $\sum_{r=0}^{r=\theta-1} \alpha_r a^{r(n-1)} + a^{t-\theta}$, where α_r is the g. c. d.* of n and $\tau(a^{t-rn})$, the different terms of the summation being the numbers of roots corresponding to the different classes of D's mentioned above.

First, $\alpha_r a^{r(n-1)}$ is the number of roots for any value of D which contains a^{nr} and no higher power of a, i. e. $D_{a^{nr}}$. For there are a^{t-r} numbers less than a^t which contain a^r, each of which may be represented by λa^r, where λ has any value less than a^{t-r}.

* Abbreviation for *greatest common divisor.*

Of course no number not included among the numbers, λa^r, can give rise to $D_{a^{nr}}$ as an n^{th}-power residue. Raising λa^r to the n^{th} power, $\lambda^n a^{nr}$, we see that its n^{th}-power residue mod. a^t is equal to the product of a^{nr} by the residue of λ^n mod. a^{t-nr}, since $a^t = a^{nr}a^{t-nr}$. That is, every n^{th} residue of mod. a^t may be decomposed in this way. If $D_{a^{nr}}$ be divided by a^{nr}, the quotient is prime to a by definition. Let H be this quotient. Then we know that $\lambda^n - H \equiv 0$ mod. a^{t-nr} has α_r roots, where $\alpha_r =$ the g. c. d. of n and $\tau(a^{t-nr})$. But if we admit all the values of λ less than a^{t-r}, there are plainly $\frac{a^{t-r}}{a^{t-nr}} = a^{r(n-1)}$ times as many roots, and this is obviously the number of roots of $X^n - D_{a^{nr}} \equiv 0$ mod. a^t.

Secondly, the last term of the sum, $a^{t-\theta}$, is the number of roots for any value of D which contains $a^{n\theta}$, i. e. for $D = 0$. This is similar to the last term of the formula in the preceding section.

For $a^t = 2^t$, n even, and $t > 2$, $\alpha_r =$ double the g. c. d. of n and $\frac{1}{2}\tau(2^{t-nr})$ [see preceding section].

For values of $n =$ or $> t$, $\theta = 1$, and the formula reduces to $\alpha + a^{t-1}$, where α is the number of roots for any value of D prime to a^t, and $a^{t-\theta}$ is the number for $D = 0$, evidently the only two classes of D's which can occur as n^{th}-power residues.

The number of roots of $X^n - D \equiv 0$ mod. $a^t b^{t'} \ldots .$ is

$$\left(\sum_{r=0}^{r=\theta-1} \alpha_r a^{r(n-1)} + a^{t-\theta}\right)\left(\sum_{r'=0}^{r'=\theta'-1} \beta_{r'} b^{r'(n-1)} + b^{t'-\theta'}\right)\ldots .$$

For simplicity let us consider a modulus of only two components, a^t, and $b^{t'}$. The proof would be the same for any number of components.

(1.) $\alpha_r\beta_{r'}a^{r(n-1)}b^{r'(n-1)}$ is the number of roots for any value of D which contains $a^{nr}b^{nr'}$. There are $a^{t-r}b^{t-r'}$ numbers less than $a^t b^{t'}$ which contain $a^r b^{r'}$, each of which may be represented by $\lambda a^r b^{r'}$, where λ is any number less than $a^{t-r}b^{t'-r'}$. No number not included by $\lambda a^r b^{r'}$ can give rise to $D_{a^{nr}b^{nr'}}$ as an n^{th}-power residue. Raising $\lambda a^r b^{r'}$ to the n^{th} power, we see that its residue mod. $a^t b^{t'}$ is equal to the product of $a^{nr}b^{nr'}$ by the residue of λ^n mod. $a^{t-nr}b^{t'-nr'}$. Let $H = \frac{D_{a^{nr}b^{nr'}}}{a^{nr}b^{nr'}}$, prime to ab by definition. Then, since $\lambda^n - H \equiv 0$ mod. $a^{t-nr}b^{t'-nr'}$ has $\alpha_r\beta_{r'}a^{r(n-1)}b^{r'(n-1)}$ roots, admitting all values of λ less than $a^{t-r}b^{t'-r'}$, it follows that the number of roots of $X^n - D_{a^{nr}b^{nr'}} \equiv 0$ mod. $a^t b^{t'}$ is the same.

(2.) $a^{t-\theta}\beta_{r'}b^{r'(n-1)}$ is the number of roots for any value of D which contains $a^{n\theta}b^{nr'}$. There are $a^{t-\theta}b^{t'-r'}$ numbers less than $a^t b^{t'}$ which contain $a^\theta b^{r'}$, and they may be represented by $\lambda a^\theta b^{r'}$ where λ has any value less than $a^{t-\theta}b^{t-r'}$. No number not included in $\lambda a^\theta b^{r'}$ can give rise to $D_{a^{n\theta}b^{nr'}}$ as an n^{th}-power residue.

Raising $\lambda a^\theta b^{r'}$ to the n^{th} power, we see that its residue mod. $a^t b^{t'}$ is equal to the product of $b^{nr'}$ by the residue of $\lambda^n a^{n\theta}$ mod. $b^{t'-nr'}$. Since $n\theta =$ or $> t$, every one of the numbers $\lambda a^\theta b^{r'}$ is a root of $X^n - D_{a^{n\theta}b^{nr'}} \equiv 0$ mod. a^t, and in order to determine how many roots there are for mod. $a^t b^{t'}$, it is necessary only to determine how many there are mod. $b^{t'}$. If $D_{a^{n\theta}b^{nr'}}$ be divided by $a^{n\theta}b^{nr}$, the quotient is prime to b by definition. Call it H. Then, since $\lambda^n - H \equiv 0$ mod. $b^{t'-nr'}$ has $a^{t-\theta}\beta_{r'} b^{r'(n-1)}$ roots for all values of λ less than $a^{t-\theta}b^{t'-r'}$, it follows that this is also the number of roots of $X^n - D_{a^{n\theta}b^{nr'}} \equiv 0$ mod. $a^t b^{t'}$.

(3.) That $b^{t'-\theta'}\alpha_r a^{r(n-1)}$ is the number of roots of $X^n - D_{a^{nr}b^{n\theta}} \equiv 0$ mod. $a^t b^{t'}$ follows by symmetry from (2).

(4.) $a^{t-\theta}b^{t'-\theta'}$ is the number of roots of $X^n - D_{a^{n\theta}b^{n\theta'}} \equiv 0$ mod. $a^t b^{t'}$, as is obvious from what has gone before. Q. E. D.

For values of $n =$ or $>$ the largest exponent in $k = a^t b^{t'} c^{t''} \ldots$, we have $\theta = 1$, and the number of roots $= (\alpha + a^{t-1})(\beta + b^{t'-1})(\gamma + c^{t''-1}) \ldots$, the same as the formula in the preceding section, there being now 2^i classes of D's, each class including one of the repetents.

§ 7. *The Number of* nth*-ic Residues.*

The different terms of $\sum_{r=0}^{r=\theta-1} \tau(a^{t-r}) + a^{t-\theta}$ evidently express, respectively, (1) the number of numbers less than and prime to a^t; (2) the number which contain a and no higher power of a; (3) the number which contain a^2 and no higher power of a; and so on to, lastly, the number of those that contain a^θ.

It is also clear that for $k = a^t b^{t'} \ldots$ the different terms of

$$\left(\sum_{r=0}^{r=\theta-1} \tau(a^{t-r}) + a^{t-\theta}\right)\left(\sum_{r'=0}^{r'=\theta'-1} \tau(b^{t'-r'}) + b^{t'-\theta'}\right)\ldots$$

express, respectively (for simplicity let us consider only two components of the modulus), (1) the number of numbers less than $a^t b^{t'}$ which contain $a^r b^{r'}$ and no higher power of either a or b; (2) the number that contain $a^\theta b^{r'}$ and no higher power of b; (3) those that contain $a^r b^{\theta'}$ and no higher power of a; (4) the number of those containing $a^\theta b^{\theta'}$.

For the modulus a^t, then, $\tau(a^{t-r})$ is the number of numbers less than a^t which contain a^r and no higher power of a, each of which, therefore, has for its n^{th}-power residue some one of the numbers that we have represented by $D_{a^{nr}}$. The formula in § 6 shows us that any n^{th}-power residue belonging to a given class occurs the same number of times. Hence, if we divide the whole number belonging to a given class by the number of times each one occurs, we obtain the number of

different residues belonging to a given class. That is, $\frac{\tau(a^{t-r})}{a_r a^{r(n-1)}}$ is the number of different n^{th}-power residues, mod. a^t, belonging to the class $D_{a^{nr}}$.

Hence, dividing $\sum_{r=0}^{r=\theta-1} \tau(a^{t-r}) + a^{t-\theta}$ by the expression in § 6 for the number of roots of $X^n - D \equiv 0$ mod. a^t, term by term, respectively, we obtain

THEOREM I. *The number of different* n^{th}*-power residues mod.* a^{t} *is* $\sum_{r=0}^{r=\theta-1} \frac{\tau(\mathrm{a}^{\mathrm{t}})}{\alpha_r \mathrm{a}^{\mathrm{rn}}} + 1$, *where* $\theta = \mathrm{E}\left(\frac{\mathrm{t}+\mathrm{n}-1}{\mathrm{n}}\right) = 1 + \mathrm{E}\left(\frac{\mathrm{t}-1}{\mathrm{n}}\right)$, *and* $\alpha_r =$ *the g. c. d. of* n *and* $\tau(\mathrm{a}^{\mathrm{t}-\mathrm{rn}})$.

In like manner, dividing the most general expression in the first part of this section by the most general expression in § 6 for the number of the roots of $X^n - D \equiv 0$ mod. $a^t b^{t'} \ldots$, we get

THEOREM II. The number of different n^{th}-power residues mod. $a^t b^{t'} \ldots$ is $\left(\sum_{r=0}^{r=\theta-1} \frac{\tau(a^t)}{a_r a^{rn}} + 1\right)\left(\sum_{r'=0}^{r'=\theta'-1} \frac{\tau(b^{t'})}{\beta_{r'} b^{r'n}} + 1\right) \ldots$.

When $n =$ or $> t$, the formula becomes $\left(\frac{\tau(a^t)}{\alpha} + 1\right)\left(\frac{\tau(b^{t'})}{\beta} + 1\right)\left(\frac{\tau(c^{t''})}{\gamma} + 1\right) \ldots$.

When $n = P(k)$ the number of n^{th} residues becomes $(1+1)(1+1)(1+1) \ldots = 2^i$, as we have already seen.

Examples. Suppose $k = 3^5 . 5^4$ to find the whole number of different cubic residues.

$$\tau(a^t) = 3^4 . 2,\ \tau(b^{t'}) = 5^3 . 4,\ \theta = E\left(\frac{5+3-1}{3}\right) = 2,\ \theta' = E\left(\frac{4+3-1}{3}\right) = 2,$$

and we have the number of cubic residues $= \left(\frac{3^4 . 2}{3} + \frac{3^4 . 2}{3 . 3^3} + 1\right)\left(\frac{5^3 . 4}{1} + \frac{5^3 . 4}{1 . 5^3} + 1\right) = 28785.$

The number of 30^{th}-power residues $= \left(\frac{3^4 . 2}{6} + 1\right)\left(\frac{5^3 . 4}{10} + 1\right) = 1428.$

That the number of n^{th}-power residues mod. k is equal to the product of the numbers for the different components of k is also readily seen from the following.

If D' be an n^{th}-power residue mod. $k = a^t b^u \ldots q^z$, then $D' \equiv a'$ mod. a^t, $D' \equiv b'$ mod. $b^u, \ldots . D' \equiv q'$ mod. q^z, where a' is some one of the n^{th}-power residues of mod. a^t, b' is some one of the n^{th}-power residues of mod. b^u, etc., etc. Then $D' \equiv a' R_{\bar{a}} + b' R_{\bar{b}} + \cdots + q' R_{\bar{q}}$. Hence the whole number of n^{th}-power residues is equal to the number of different ways of combining the different numbers represented by a' with those represented by $b', c', \ldots . q'$, that is to say, is equal to the product of the numbers of n^{th}-power residues for the different components of k, a^t, b^u, etc. No two values of D thus obtained will be congruous to each other [§ 2, Theorem VIII.]. If $s = ab \ldots l$, the different s-totitive n^{th}-power resi-

dues mod. k will be obtained by combining, according to the formula, the different n^{th}-power residues mod. a^t which are a-totitives of a^t, with the different n^{th}-power residues mod. b^u which are b-totitives of b^u, ... with those mod. l^x which are l-totitives of l^x, with those mod. m^y which are prime to m^y, ... with those mod. q^z which are prime to q^z. That is, the number of n^{th}-power residues mod. k which are s-totitives of $k = A'B'. \ldots . L'M \ldots . Q$, where $A', B', \ldots . Q$, represent respectively the different numbers described above. We have seen that the whole number of n^{th}-power residues mod. $a^t = \sum_{r=0}^{r=\theta-1} \frac{\tau(a^t)}{a_r a^{rn}} + 1$. That is, $A = \frac{\tau(a^t)}{a}$, and $A' = \sum_{r=1}^{r=\theta-1} \frac{\tau(a^t)}{a_r a^{rn}} + 1$, and so on for B, B', C, C', etc. Then the *whole* number of n^{th}-power residues mod. $k = a^t b^u \ldots . q^z$ is $(A + A')(B + B') \ldots . (Q + Q')$, where each term of the expansion denotes the number of residues belonging to that class of totitives of k whose subscript corresponds to the accented letters in the term. Thus the number of n^{th} residues which are ap-totitives of k is $A'BC \ldots . P'Q$.

§ 8. *The Junction of Fermat's and Wilson's Theorems.*

We know from the theory of indices [see Dirichlet's *Zahlentheorie*, § 30] that if $k = a^t$, $2a^t$, or 4, where a is an odd prime number, the $\frac{\tau(k)}{\delta}$ δ^{th}-power residues of mod. k which are prime to k are congruous to $g^\delta, g^{2\delta}, \ldots . g^{\frac{\tau(k)}{\delta}\delta}$, where δ is a divisor of $\tau(k)$, and g is any primitive root of k. Hence, if x' be any one of the δ roots of $x^\delta \equiv g^\delta$ mod. k, and x'' any one of the δ roots of $x^\delta \equiv g^{2\delta}$ mod. k, etc., etc., we have the following: —

THEOREM I. $\left(x'x'' \ldots . x^{\left[\frac{\tau(k)}{\delta}\right]}\right)^\delta \equiv \left(-1\right)^{\frac{\tau(k)}{\delta}+1}$ *mod.* k, *where* $k = a^t, 2a^t,$ *or* 4.

For, by multiplying together the congruences $x^\delta \equiv g^\delta$, $x^\delta \equiv g^{2\delta}$, etc., mod. k, we get

$$\left(x'x'' \ldots . x^{\left[\frac{\tau(k)}{\delta}\right]}\right)^\delta \equiv g^{\frac{\tau(k)}{2}\left(\frac{\tau(k)}{\delta}+1\right)} \equiv \left(-1\right)^{\frac{\tau(k)}{\delta}+1} \text{ mod. } k,$$

since $g^{\frac{\tau(k)}{2}} \equiv -1$ mod. k. Q. E. D. This is only another form of the well-known theorem that the product of the δ^{th} power residues is congruous to $(-1)^{\frac{\tau(k)}{\delta}+1}$ mod. k. [See Gauss, D. A., § 75]. This theorem becomes Fermat's when $\delta = \tau(k)$, for we then have $x^{\tau(k)} \equiv 1$ mod. k; and when $\delta = 1$ we have $(x'x'' \ldots . x^{[\tau(k)]}) \equiv -1$ mod. k, which is Wilson's theorem. It may be remarked that there are $\delta^{\frac{\tau(k)}{\delta}}$ different combinations of numbers less than k which satisfy the congruence of this theorem. Instead of -1 we may write $-R_1$.

For completeness I state what is obvious for $k = a^t$, viz. $\left(x'x''.\ldots x^{\left[\frac{\tau_a(k)}{\delta}\right]}\right)^{\delta} \equiv -R_a \equiv 0 \bmod k$, where $x', x'', \ldots$ are a-totitives of k, and this of course holds when $a = 2$. But if $a = 2\,x', x''$, etc., be odd, we have

THEOREM II. If $k = 2^t$, $t > 2$, and δ be any divisor of $\tau(k)$, then

$$\left(x'x''.\ldots x^{\left[\frac{\tau(k)}{\delta}\right]}\right)^{\delta} \equiv 1 \bmod k.$$

For δ must be unity or some power of 2. When $\delta = 1$ the theorem becomes Wilson's theorem. When $\delta =$ a power of 2, we know that the $\frac{1}{2}\frac{\tau(k)}{\delta}$ δ^{th}-power residues which are prime to k are congruous to $g^{\delta}, g^{2\delta}, \ldots . g^{\frac{1}{2}\frac{\tau(k)}{\delta}}$, where g is some one of those roots of $x^{\frac{1}{2}\tau(k)} \equiv 1 \bmod k$ which are not roots of a similar congruence of a less degree. Hence, if x' be any one of the 2δ roots of $x^{\delta} \equiv g_{\delta} \bmod k$ [see Serret's *Cours d'Algèbre Supérieure*, § 324], x'' any other root of the same congruence, x''' any one of the 2δ roots of $x^{\delta} \equiv g^{2\delta} \bmod k$, x^{IV} any other root of the same congruence, etc., etc., we have by multiplication

$$\left(x'x''.\ldots x^{\left[\frac{\tau(k)}{\delta}\right]}\right)^{\delta} \equiv g^{2\delta}g^{4\delta}g^{6\delta}.\ldots g^{\frac{\tau(k)}{\delta}\delta} \equiv g^{\frac{\tau(k)}{2}\left(\frac{\tau(k)}{2\delta}+1\right)} \equiv 1 \bmod k,$$

since $g^{\frac{\tau(k)}{2}} \equiv 1 \bmod k$. Q. E. D. For $\delta = \tau(k)$ this becomes Fermat's theorem.

We can now prove the most general form of these theorems, bringing together the extended Fermat's and Wilson's theorems given in § 3.

THEOREM III. If $k = a^t b^u.\ldots q^z$, and $\Delta =$ any divisor of $\tau\left(\frac{k}{\sigma}\right)$, then $\left(X_s'X_s''.\ldots X_s^{\left[\frac{\tau_s(k)}{\Delta}\right]}\right)^{\Delta} \equiv R_s \bmod k$; except when $\frac{k}{\sigma} = q^z$, $2q^z$, or $= 4$, and $\frac{\sigma}{s}$ is at the same time an odd number, in which cases

$$\left(X_s'X_s''.\ldots X_s^{\left[\frac{\tau_s(k)}{\Delta}\right]}\right)^{\Delta} \equiv (-R_s)^{Q+1} \bmod k,$$

where Q is the number of the Δ^{th}-power residues of mod. q^z, mod. $2q^z$, or mod. 4, which are prime to the modulus. X_s', X_s'', etc., will be defined below.

If $s = ab.\ldots l$, we have seen that the number of Δ^{th}-power residues mod. k which are s-totitives of k is $A'B'.\ldots L'M.\ldots Q$ [close of preceding section], where A' is the number of the Δ^{th}-power residues mod. a^t which contain a, $\ldots . M$ is the number of those mod. m^y which are prime to m, etc., etc. Put $A'B'.\ldots Q = \Omega$. When $\Delta = 1$, $\Omega = \tau_s(k)$, and when $\Delta =$ or $>$ the largest exponent in σ, $\Omega = M.\ldots Q = \omega$, for brevity.

We have seen that, if D_s' be a Δ^{th}-power residue mod. k, $D_s' \equiv a'R_{\bar{a}} + b'R_{\bar{b}} + \ldots . + q'R_{\bar{q}} \bmod k$, where a' is any Δ^{th}-power residue mod. a^t, etc., etc., for

$b', \ldots, q'$. Give a^{t-1} values to a', i. e. all its A' distinct values and $a^{t-1} - A'$ repetitions to make up the number to a^{t-1}. Give b^{u-1} values to $b', \ldots,$ l^{x-1} values to l' in the same way. Give to $m', \ldots, q'$, their $M, \ldots, Q$, distinct values, respectively. We shall thus get $\frac{\sigma}{s}\omega$ values of D'_s, including among them the Ω distinct values of D'_s. We know that there are ω incongruous values of D'_s mod. $\frac{k}{\sigma}$. Represent the product of these $\frac{\sigma}{s}\omega$ values of D'_s by ΠD_s. Then we have [see Theorem I. and § 2, Theorem VI.],

$$\Pi D_s \equiv \left(m'm'' \ldots . m^{[M]}\right)^{\frac{\sigma}{s}N \ldots . Q} R_{\bar{m}} + \ldots . + \left(q'q'' \ldots . q^{[Q]}\right)^{\frac{\sigma}{s}M \ldots . P} R_{\bar{q}} \text{ mod. } k,$$

$$\therefore \Pi D_s \equiv \left(-1\right)^{(M+1)\frac{\sigma}{s}N \ldots . Q} R_{\bar{m}} + \ldots . + \left(-1\right)^{(Q+1)\frac{\sigma}{s}M \ldots . P} R_{\bar{q}} \text{ mod. } k,$$

by Theorem I., whence if $\frac{\sigma}{s}$ be even, or if any two of the numbers $M, \ldots, Q$, be even, or if they be all odd, we have $\Pi D_s \equiv R_{\bar{m}} + \ldots . + R_{\bar{q}} \equiv R_{\overline{m \ldots . q}} = R_s$ [see § 2, Formula (C)]. In any case, we have

$$(\Pi D_s)^2 \equiv R_{\bar{m}} + \ldots . + R_{\bar{q}} \equiv R_{\overline{m \ldots . q}} = R_s \text{ mod } k.$$

If one, and only one, of the numbers $M, \ldots, Q$ be even, Δ is even, since $\tau(m^y)$, $\ldots, \tau(q^z)$, are even. Hence we have $\frac{\tau_s(k)}{\Delta} \div \frac{\sigma}{s}\omega = \frac{\mu \ldots . \chi}{\Delta} = \epsilon$, for brevity, = an even number. For $M = \frac{\tau(m^y)}{\mu}, \ldots, Q = \frac{\tau(q^z)}{\chi}$, where μ is the g. c. d. of Δ and $\tau(m^y)$, etc., etc., and if M, for instance, be the one that is even, μ will contain as high a power of 2 as Δ, while $\nu, \ldots, \chi$, will each contain at least the first power of 2, since the numbers which they divide are even.

Hence, if $D'_s, D''_s, \ldots, D_s^{[\Omega]}$, be the Ω distinct Δ^{th}-power residues mod. k which are s-totitives of k, and X'_s be any one of the roots of $X_s^\Delta \equiv D'_s$ mod. k, X''_s any one of the roots of $X_s^\Delta \equiv D''_s$ mod. k, etc., to $X_s^{[\Omega]}$ any one of the roots of $X_s^\Delta \equiv D_s^{[\Omega]}$ mod. k, and if $\frac{\sigma}{s}\omega - \Omega$ more roots be chosen in any way from these congruences, provided that $\frac{\sigma}{s} - \frac{\Omega}{\omega}$ be taken from each of the ω classes of congruences which are distinct with reference to the modulus $\frac{k}{\sigma}$, then, according to what has just been proved, we have by multiplication,

$\left(X'_s X''_s \ldots . X_s^{\left[\frac{\sigma}{s}\omega\right]}\right)^\Delta \equiv \Pi D_s \equiv R_s$ mod. k, provided $\frac{\sigma}{s}$ is even, or at least two of the quantities $M, \ldots, Q$, are even, or if they are all odd. If these conditions be not fulfilled, then, since in this case ϵ is even, we may duplicate

the numbers X_s', X_s'', etc., taking each duplicate from the roots of the same congruence from which X_s', X_s'', etc., were taken respectively, and then have

$$\left(X_s'X_s''\ldots.X_s^{\left[2\frac{\sigma}{s}\omega\right]}\right)^{\Delta} \equiv (\Pi D_s)^2 \equiv R_s \text{ mod. } k.$$

If, now, $\epsilon > 1$ in the first case and $\frac{\epsilon}{2} > 1$ in the second case, we have, by an ϵ-fold reduplication of the numbers, X_s', X_s'', etc., where the roots taken from any particular one of the congruences may be the same or different,

$$\left(X_s'X_s''\ldots.X_s^{\left[\frac{\tau_s(k)}{\Delta}\right]}\right)^{\Delta} \equiv R_s \text{ mod. } k, \text{ since } R_s^n \equiv R_s.$$

This proves the theorem outside of the excepted cases, and these let us now consider.

For $\frac{k}{\sigma} = q^z$, we have, in the same way as before,

$$\Pi D_s \equiv \left(q'q''\ldots.q^{[Q]}\right)^{\frac{\sigma}{s}} R_{\bar{q}} \equiv \left(-1\right)^{(Q+1)\frac{\sigma}{s}} R_{\bar{q}} \equiv R_{\bar{q}} \equiv R_s \text{ mod. } k,$$

where $\frac{\sigma}{s}$ is even; otherwise $\equiv (-R_s)^{Q+1}$ mod. k.

For $\frac{k}{\sigma} = 4$, we have $\Pi D_s \equiv \left(-R_{\bar{2}}\right)^{(Q+1)\frac{\sigma}{s}} \equiv \left(-R_s\right)^{(Q+1)\frac{\sigma}{s}}$, as before.

For $\frac{k}{\sigma} = 2q^z$, we get, in the same way as before,

$$\Pi D_s \equiv \left(h'h''\ldots.h^{[H]}\right)^{\frac{\sigma}{s}Q} R_{\bar{2}} + \left(q'q''\ldots.q^{[Q]}\right)^{\frac{\sigma}{s}H} R_{\bar{q}} \text{ mod. } k.$$

But since $\tau(2) = 1$, $H = 1$, and h', the Δ^{th}-power residue mod. 2 which is prime to 2, is also $= 1$. Hence, we have here $\Pi D_s \equiv R_{\bar{2}} + \left(-1\right)^{(Q+1)\frac{\sigma}{s}} R_{\bar{q}}$ mod. k. When $k =$ twice an odd number, as in this case, we have plainly $R_{\bar{2}} = \frac{1}{2}k$, for $\frac{1}{2}k$ contains all the components of k except 2. Hence $R_{\bar{2}} \equiv -R_{\bar{2}}$ mod. k. Hence, since $\frac{\sigma}{s}$ is odd, we have

$$\Pi D_s \equiv (-R_{\bar{2}} - R_{\bar{q}})^{Q+1} \equiv (-R_{2\bar{q}})^{Q+1} \equiv (-R_s)^{Q+1} \text{ mod. } k.$$

In these excepted cases $\epsilon = \frac{\chi}{\Delta} = 1$, since Δ is any divisor of $\tau\left(\frac{k}{\sigma}\right)$, i. e. $\tau(q^z)$, or $\tau(2q^z)$, or $\tau(4)$, and χ is the g. c. d. of Δ and $\tau(q^z)$, or $\tau(4)$. Hence $\frac{\tau_s k}{\Delta} = \frac{\sigma}{s}\omega$, and we have proved $\left(X_s'X_s''\ldots.X_s^{\left[\frac{\tau_s(k)}{\Delta}\right]}\right)^{\Delta} \equiv (-R_s)^{Q+1}$ mod. k, for the excepted

cases, the theorem being obvious when $\frac{k}{\sigma} = 1$, and for the non-excepted cases $\left(X_s' X_s'' \ldots . X_s^{\left[\frac{\tau_s(k)}{\Delta}\right]}\right)^{\Delta} \equiv R_s \bmod. k$. Q. E. D.

For $\Delta = 1$, we have the extended form of Wilson's theorem given in § 3.

For $\Delta = \tau\left(\frac{k}{\sigma}\right)$, we have $\left(X_s' X_s'' \ldots . X_s^{\left[\frac{\sigma}{s}\right]}\right)^{\tau\left(\frac{k}{\sigma}\right)} \equiv R_s$ or $(-R_s)^{Q+1}$, and since Ω in this case $= 1$, the numbers X_s', X_s'', etc., are all roots of $X_s^{\Delta} \equiv R_s$ mod. k. Hence we have $X_s^{\frac{\sigma}{s}\tau\left(\frac{k}{\sigma}\right)} \equiv R_s$, since $Q = 1$. Hence $X_s^{\tau_s(k)} \equiv R_s$ mod. k, the Fermatian theorem of § 3. Although the theorems of § 3 are included in the above theorem, it seemed best, for the sake of simplicity and clearness, to prove the special cases first.

SCHOLIUM. If $\Pi' D_s$ denote the product of all the Ω distinct n^{th}-power residues which are s-totitives of k, the above method of proof shows that $\Pi' D_s \equiv R_s$ mod. k if all the numbers $M, \ldots ., Q$, be odd, or if at least two be even. In any case we have $(\Pi' D_s)^2 \equiv R_s$ mod. k.

It may be proved that, if $X^{\Delta} \equiv D$ mod. k, then $D^{\frac{P(k)}{\Delta}} \equiv R$ mod. k, where R denotes an undistinguished repetent. The proof is exactly the same as that of the ordinary theorem for prime moduli [Serret, *Alg. Sup.*, § 310], and need not be repeated here. The reciprocal of this does not hold, in general, for composite moduli. That is, it is not true, in general, that all the roots of $X^{\frac{P(k)}{\Delta}} - R \equiv 0$ mod. k are Δ^{th}-power residues, as may be easily seen. A brief consideration of the case where $\Delta = 2$ will close the present paper. We know that $X^{P(k)} - R \equiv 0$, or $(X^{\frac{P(k)}{2}} - R)(X^{\frac{P(k)}{2}} + R) \equiv 0$ mod. k, has k roots. All the quadratic residues of mod. k are roots of the first factor; the non-quadratic residues may be roots of either factor, or of neither, i. e. may be roots of the product of the two factors. For the particular case where the prime factors of k are each of the first degree, and of the form $2^c(2^r + 1) + 1$, where c is constant and r variable, application of the formulæ of § 5 and § 7 shows us that the number of roots of $X^{\frac{P(k)}{2}} - R \equiv 0$ mod. k is the same as the number of the quadratic residues mod. k, viz.: $[2^{c-1}(2^r + 1) + 1][2^{c-1}(2^{r'} + 1) + 1] \ldots .$ So that in this case, just as in the case of prime moduli, all the roots of $X^{\frac{P(k)}{2}} - R \equiv 0$ mod. k are quadratic residues, and *vice versa*.